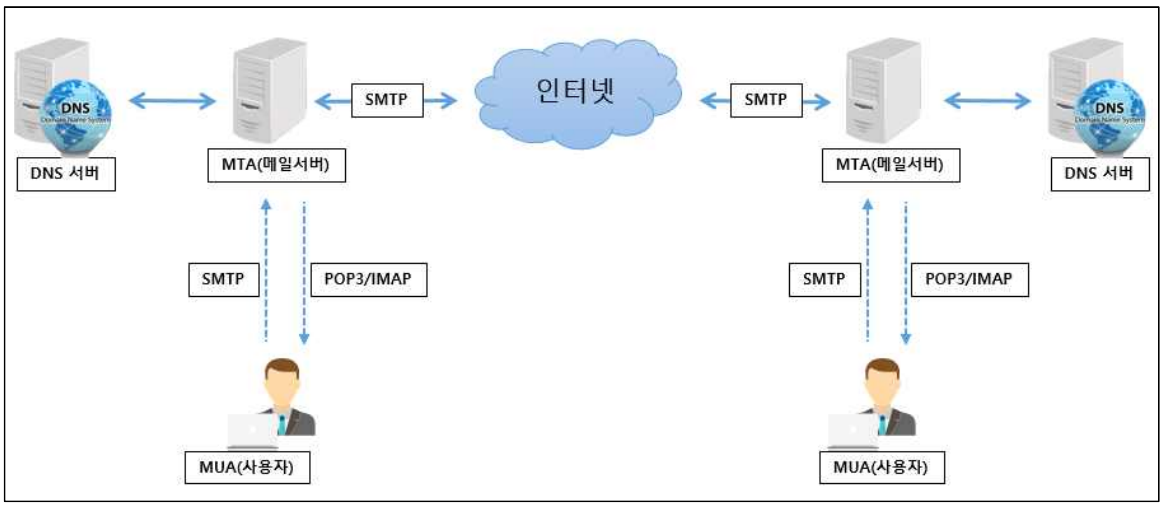
참고 이메일 구성 요소 및 보안인증기술

□ 이메일 송·수신을 위한 구성요소



o 메일 사용자 에이전트(MUA)

- 사용자가 E-mail을 읽고 답장하고 삭제할 수 있는 프로그램으로 사용하는 Outlook Express(아웃룩)등의 클라이언트 소프트웨어

o 메일 전송 에이전트(MTA)

- MUA에서 작성되고 전송된 E-mail을 처리하는 역할로 메일서버가 MTA에 해당함

□ **이메일 전송 프로토콜**

o SMTP(Simple Mail Transfer Protocol)

- E-mail을 전달시켜 주는 프로토콜로 기본으로 TCP 25 포트를 사용하며, PC에서 메일서버로 메일을 보낼 때, 메일서버끼리 메일을 주고 받을 때 사용

o POP3/ IMAP

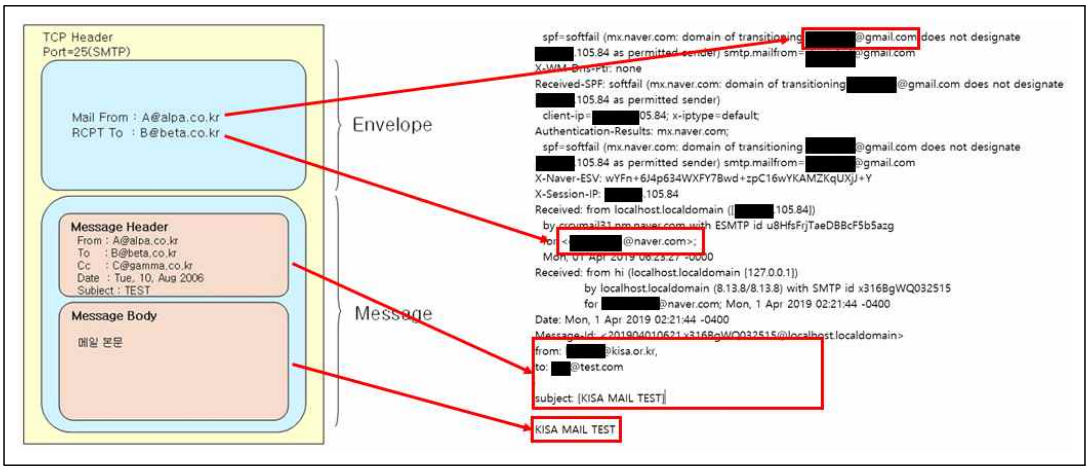
- 메일 서버로부터 메일을 검색하여 MUA로 메일을 가져올 때 사용

□ 메일 표준 포맷 및 구조별 역할

o 메일의 표준 포맷(RFC822)

- 메일의 표준 포맷은 봉투(Envelope)와 메시지(Message) 부분으로 이루어져 있음

<메일의 표준 포맷 및 실제 메일 헤더>



<실제 메일 수신 화면>

o 봉투(Envelope)와 메시지(Message)의 역할

- 봉투의 역할은 사용자와 메일서버 사이에서 통신을 위한 용도로 사용(수신자, 발신자 주소가 포함)
- 메시지의 역할은 사용자가 메일을 받아 실제 메일 프로그램에서 보여주는 역할로 사용(수신자, 발신자, 참조, 날짜, 제목, 본문 등이 포함)

☞ **봉투에 적힌 발신자와 메시지에 적힌 발신자가 다를 수 있음**

□ 메일서버등록제(SPF, Sender Policy Framework, RFC4408)

o 이메일 수신측에서 발신측이 정상적으로 등록된 서버인지를 확인하여 정상메일 여부를 식별할 수 있도록 지원하는 대표적인 인증기술

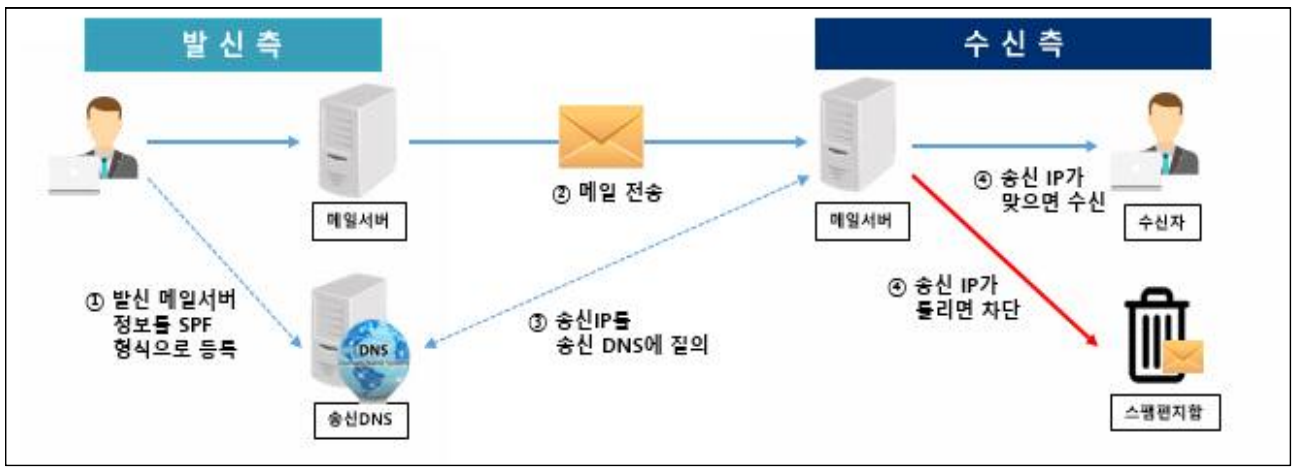
- **(발신측)** 사전에 발신 메일서버의 정보(IP)와 메일정책을 자신의 DNS에 SPF 레코드 형식으로 등록

※ SPF 정책은 DNS TXT 리소스 레코드에만 인코딩되므로 발신측은 특수 소프트웨어가 필요하지 않음

- **(수신측)** 메일 발신자 도메인에 대해 도메인 서버에 기록된 SPF 레코드를 조회/확인 하고, 결과값에 따라 메일의 수신여부 결정

※ 수신측은 SPF 정책을 확인할 수 있는 기능 필요

o 메일서버등록제 활용 절차



① **(설정 단계)** 이메일 발신측은 DNS에 사전에 메일서버 정보를 TXT 레코드로 등록

② **(전송 단계)** 발신측이 수신측으로 이메일 전송

③ **(확인 단계)** 이메일 수신측에서 발신측 DNS TXT의 SPF 레코드를 참조 하여 SPF 인증 통과 여부 판정

□ 도메인키인증메일(DKIM, Domain Keys Indentified Mail, RFC4871)

o 이메일 수신측에서 발신 도메인의 위변조 여부를 확인하여 정상메일 여부를 식별할 수 있도록 지원하는 발신 도메인 인증기술

※ DKIM 서명은 메시지 본문을 포함하기 때문에 이메일 통신의 무결성도 보호

- **(발신측)** 사전에 자신의 DNS에 공개키를 등록하고, 메일을 보낼 때 자신의 개인키로 전자서명하여 전송

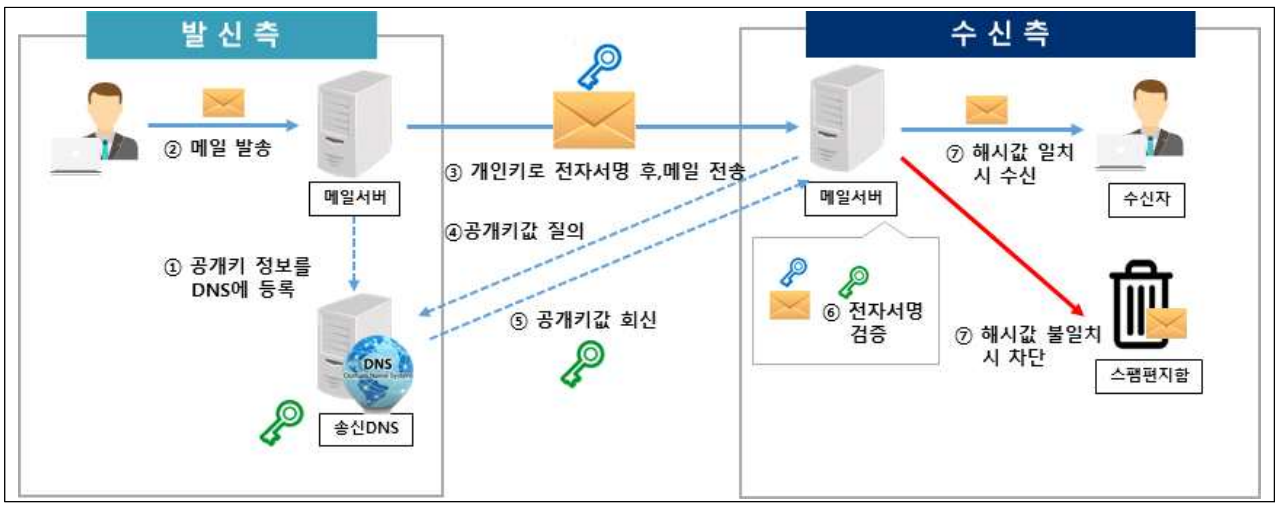
※ 기업의 DNS에 공개키가 존재한다는 것은 기업과 송신자 사이에 관계가 있음을 의미

※ 송신자 MTA에 DKIM 서명을 생성할 수 있는 기능 필요

- **(수신측)** 수신메일에 지정된 DNS로부터 얻은 공개키로 해시값을 비교하여 수신여부 결정

※ 수신자 MTA에 DKIM 서명을 확인할 수 있는 기능 필요

o 도메인키인증메일 활용 절차



① **(설정 단계)** 이메일 발신측은 DNS에 사전에 공개키 정보를 TXT 레코드로 등록

② **(전송 단계)** 발신측이 개인키로 전자서명 후, 수신측으로 이메일 전송

③ **(확인 단계)** 이메일 수신측에서 발신측 DNS TXT의 공개키 획득 후, 전자서명 검증을 통해 DKIM 인증 통과 여부 판정

□ 도메인기반 이메일 인증

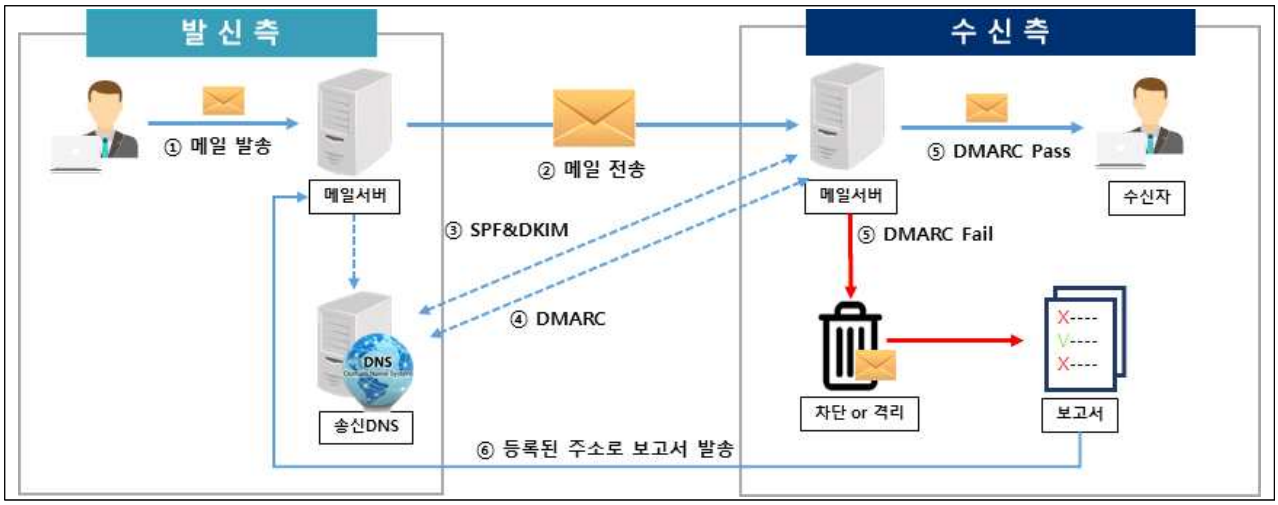
(DMARC, Domain-Based Message Authentication, Reporting & Conformance, RFC7489)

o SPF, DKIM의 검사 결과를 기초로 TXT 레코드의 내용에 따라 메일 발송 차단, 혹은 자신의 메일 도메인을 도용한 스푸핑 메일에 대한 보고 등 설정

- **(발신측)** SPF 또는 DKIM 또는 둘 모두를 구축, 발신되는 메시지를 처리하는 방법을 수신자에게 알려주기 위해 DNS에 DMARC 정책을 게시
- **(수신측)** DNS에서 SPF, DKIM 및 DMARC 레코드를 검색하고 여기에 인코딩된 정책에 따라 동작

※ 수신자 MTA에 SPF 정책, DKIM 서명, DMARC 정책을 확인하고 DMARC 정책 처리 결과 피드백을 위한 보고서 생성 기능 필요

o 도메인기반 인증·레포팅·적합성 활용 절차



① **(설정 단계)** 이메일 발신측은 DNS에 사전에 DMARC 설정을 TXT 레코드로 등록

② **(전송 단계)** 발신측이 수신측으로 이메일 전송

③ **(확인 단계)** 이메일 수신측에서 발신측 DNS TXT의 DMARC 정책을 참조하여 인증 통과 여부 판정